UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,892	08/10/2006	Naoto Kuroda	9319Y-1322/NP	7169

27572 7590 04/27/2009

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/549,892	KURODA, NAOTO	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-7,9-13,15-18,20 and 21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 4-7, 9-13, 15-18, 20, and 21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is response to Amendment filed 2/6/2009. Claims 1, 4-6, 9-11, 15-18, 20, and 21 are amended. Claims 3, 8, 14, and 19 have been cancelled. Claims 1, 2, 4-7, 9-13, 15-18, 20, and 21 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 2, 4-7, 9-13, 15-18, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al (US Patent No. 5,440,723 and Arnold hereinafter) in view of Bar et al. (US Patent Publication No. 2005/0021740 and Bar hereinafter).

2. As to claim 1, Arnold teaches a method of preventing virus infection performed by a computer connected to a network comprising steps of: obtaining communication information when a virus intrudes into the computer (e.g., data processing system) (i.e., ... teaches obtaining virus signature information [col. 9, lines 10-20] … teaches Periodic monitoring of the data processing system 10 for anomalous, potentially virus-like behavior [col. 2, lines 50-56) … further teaches If preliminary evidence of virus-like

activity is detected, additional computational resources are devoted to obtaining more conclusive evidence of viral infection [col. 5, lines 29-32]);

detecting a virus source computer based on the communication information obtained (i.e., ... teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]);

sending a message announcing an antivirus attack on the virus source computer [fig. 3, (E)];

and making the antivirus attack on the virus source computer from the computer by imposing a high load on the virus source computer [fig. 5, Block A-E].

Arnold does not expressly teach the claim limitation element imposing a high load on the virus source computer. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Arnold as introduced by Bar. Bar discloses the claim limitation element imposing a high load on the virus source computer (to provide blocking (e.g., high load) capability on traffic sent from a infectious computing system [par. 82]):

Therefore, given the teachings of Bar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Arnold by employing the well known feature of blocking traffic for a infectious system disclosed above by Bar, for which preventing virus infection will be enhanced (par. 82).

3. As to claim 2, Arnold teaches a method of preventing virus where: a decoy accessible through the network is provided to a computer that monitors intrusion of a virus (i.e., ... teaches deploying a decoy to capture virus [item C, fig. 2]), for receiving access to said decoy to obtain communication information and to detect virus intrusion (i.e., ... teaches the DPs are periodically compared to the secured copies stored within the DPDB 76a so as to detect a modification thereof [col. 29, lines 8-12]); and said decoy is one or more of a decoy folder stored in a storage unit, a decoy application stored in the storage unit (i.e., teaches the decoy program unit 76 has an associated secure decoy program database (DPDB) 76a [col. 29, lines 1-10]), and a server formed virtually in the storage unit (i.e., ... although silent on the term "server", those ordinary skill in the art would recognize the teaching of the DPs are periodically compared to the secured copies stored within the DPDB 76a so as to detect a modification thereof. If a modification is detected, the DPU 76 isolates the undesirable software entity and provides one or more samples of the isolated undesirable software entity to the code/data segregator 38 [col. 29, lines 8-16]).

4. As to claim 3 and 8 (cancelled)

5. As to claim 4 and 9, Arnold teaches a method of preventing virus infection where: said high load is imposed on the virus source computer by increasing traffic of said computer (i.e., ... teaches anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse [col. 4, lines 30-35]).

6. As to claim 5 and 10, Arnold teaches a method of preventing virus infection where: said high load is imposed on the virus source computer by sending a large number of requests to which a CPU of said computer should respond (i.e., ... teaches anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse [col. 4, lines 30-35]).

7. As to claim 6, Arnold teaches a system for preventing virus infection formed on a computer connected to a network, comprising:

a communication information analysis means that detects intrusion of a virus, and then on detecting virus intrusion into the computer (e.g., data processing system) (i.e., ... teaches obtaining virus signature information [col. 9, lines 10-20] … teaches Periodic monitoring of the data processing system 10 for anomalous, potentially virus-

like behavior [col. 2, lines 50-56) … further teaches If preliminary evidence of virus-like activity is detected, additional computational resources are devoted to obtaining more conclusive evidence of viral infection [col. 5, lines 29-32]), detects a virus source computer based on communication information obtained when the virus intrudes (i.e., ... teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]);

a computer attack means that makes an antivirus attack on the virus source computer through the network from the computer for suppressing operation of the virus (i.e., … teaches user is informed of suspicious activity and given a choice as to whether to continue running or to suspend the offending process (and/or the family tree of processes to which it is related) pending further investigation. … further teaches If the user chooses to suspend the process, the method proceeds to Step B, in which that process, all parents or children of that process, and perhaps all other processes in memory, are scanned for known worms. Cleanup involves killing active worm processes (determined by tracing the process tree), and deleting worm executables and auxiliary files from storage media. Backup of files is not likely to be as necessary in this

case, as it is for viruses, since a worm typically does not alter other executables [col. 21, lines 25-40]);

and a message sending means that sends a message for announcing a start of the attack, to the infected computer (i.e., ... teaches a distress signal deployment [col. 20, Step G])

Arnold does not expressly teach the claim limitation element of computer attack means imposes a high load on the virus source computer. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Arnold as introduced by Bar. Bar discloses the claim limitation element of computer attack means imposes a high load on the virus source computer (to provide blocking (e.g., high load) capability on traffic sent from a infectious computing system [par. 82]):

Therefore, given the teachings of Bar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Arnold by employing the well known feature of blocking traffic for a infectious system disclosed above by Bar, for which preventing virus infection will be enhanced (par. 82).

8. As to claim 7, Arnold teaches a system for preventing virus infection where: said system further comprises a decoy means accessible through the network [fig. 2, (C)];

and said communication information analysis means detects virus intrusion into said decoy means, and on detection of the virus intrusion [fig. 3, (J)], detects a virus

source computer, based on the communication information obtained when the virus intrudes (i.e., ... teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]).

9. As to claim 11, Arnold teaches a system for preventing virus infection where; and said computer attack means continues to make the antivirus attack on the virus source computer until a countermeasure against the virus has been completed [fig. 5, block A-E].

10. As to claim 12, Arnold teaches a system for preventing virus infection where said decoy means is a decoy folder realized by an application provided in a decoy server that is formed virtually in a storage unit of a computer connected to the network (... teaches added as a dedicated decoy program server [col. 4,lines 25-30]).

11. As to claim 13, Arnold teaches a system for preventing virus infection where: said decoy means is a decoy application realized as an application provided in a decoy server that is formed virtually in a storage unit of a computer connected to the network

(i.e., ... teaches Deployment of decoy programs to capture virus samples [col. 4, Step C] ... teaches one or more decoy programs in an attempt to attract and obtain one or more samples of the unknown virus. The decoy programs could be commercially- available computer programs which are installed on (and are capable of being executed on) the computer system [col. 6, lines 5-15] ... teaches added as a dedicated decoy program server [col. 4,lines 25-30]).

12. Claim 14. (cancelled)

13. As to claim 15, Arnold teaches a system for preventing virus infection further comprising: an alarm sound generation means that generates an alarm sound in an attacking terminal unit at a start of the attack or after the start of the attack (i.e., ... teaches deployment of a distress signal [col. 20, Step G]).

14. As to claim 16, Arnold teaches a system for preventing virus infection further comprising: a requesting means that notifies a network address of the virus source computer to another computer connected to the network and requests to said computer for making an antivirus attack on the virus source computer (i.e., ... teaches alerting neighboring computers [abstract (F)] ... teaches performing antivirus processing [fig. 8] ... although silent on the term "request" for making the antivirus attack those skill in the art would recognize upon invoking the process to execute performing antivirus

processing in [fig. 8] a triggering process such as a request process would have had to occur for in order for the [fig. 8] processes to execute).

15. As to claim 17, Arnold teaches a system for preventing virus infection formed on a computer (e.g., decoy server) connected to a network, comprising:

a request receiving means that receives a request for making an antivirus attack on a virus source computer ... teaches performing antivirus processing [fig. 8] ... although silent on the term "request" for making the antivirus attack those skill in the art would recognize upon invoking the process to execute performing antivirus processing in [fig. 8] a triggering process such as a request process would have had to occur for in order for the [fig. 8] processes to execute);

and a computer attack means in the computer that makes an antivirus attack on said virus source computer through the network for suppressing operation of a virus, based on said request received (i.e., … teaches user is informed of suspicious activity and given a choice as to whether to continue running or to suspend the offending process (and/or the family tree of processes to which it is related) pending further investigation. … further teaches If the user chooses to suspend the process, the method proceeds to Step B, in which that process, all parents or children of that process, and perhaps all other processes in memory, are scanned for known worms. Cleanup involves killing active worm processes (determined by tracing the process tree), and deleting worm executables and auxiliary files from storage media. Backup of

files is not likely to be as necessary in this case, as it is for viruses, since a worm typically does not alter other executables [col. 21, lines 25-40]).

16. As to claim 18, Arnold teaches a program stored on a computer readable medium that is read into a computer connected to a network and makes the computer operate to prevent virus infection (e.g., decoy server), wherein: the program makes said computer realize: a communication information analysis means that detects intrusion of a virus, and then on detecting virus intrusion, detects a virus source computer based on communication information obtained when the virus intrudes (i.e., ... teaches The first step in the process of this invention detects anomalous system behavior of a type that may indicate the presence of an undesirable informational state resulting from the presence of a virus or some other undesirable software entity, such as a worm or a Trojan Horse. The detection of anomalous behavior within a computer or computer network can be accomplished through the use of known techniques, preferably a technique that detects anomalies that may indicate a virus [col. 4, lines 60-69; col. 5, lines 1-5]):

a computer attack means that makes an antivirus attack on the virus source computer from the computer through the network, for suppressing operation of the virus (i.e., … teaches user is informed of suspicious activity and given a choice as to whether to continue running or to suspend the offending process (and/or the family tree of processes to which it is related) pending further investigation. … further teaches If the user chooses to suspend the process, the method proceeds to Step B, in which that

process, all parents or children of that process, and perhaps all other processes in memory, are scanned for known worms. Cleanup involves killing active worm processes (determined by tracing the process tree), and deleting worm executables and auxiliary files from storage media. Backup of files is not likely to be as necessary in this case, as it is for viruses, since a worm typically does not alter other executables [col. 21, lines 25-40]);

and a message sending means that sends a message for announcing a start of the attack, to the infected computer (i.e., ... teaches the deployment of a distress signal [col. 20, Step G].

Arnold does not expressly teach the claim limitation element of computer attack means imposes a high load on the virus source computer. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Arnold as introduced by Bar. Bar discloses the claim limitation element of computer attack means imposes a high load on the virus source computer (to provide blocking (e.g., high load) capability on traffic sent from a infectious computing system [par. 82]):

Therefore, given the teachings of Bar, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Arnold by employing the well known feature of blocking traffic for a infectious system disclosed above by Bar, for which preventing virus infection will be enhanced (par. 82).

17. Claim 19. (cancelled)

18. As to claim 20, Arnold teaches a system for preventing virus infection comprising: and an alarm sound generation means the generates an alarm sound in an attacking terminal unit at a start of the attack or after the start of the attack (i.e., ... teaches the deployment of a distress signal [col. 20, Step G]).

19. As to claim 21, Arnold teaches a system for preventing virus infection comprising: a detection report transmission means that sends a detection report to an administrator of the virus source computer (i.e., … teaches situation is noted in the report at Block P [fig. 3]).

Response to Arguments

Applicant's arguments with respect to claims 1, 2, 4-7, 9-13, 15-18, 20, and 21 have been considered but are moot in view of the new ground(s) of rejection. Examiner contends the teachings of Bar provides for the capability to block (e.g., imposing a high load) communication to suspend an attack from a suspected infectious computer system [par. 82]).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431